The Legal Intelligencer

THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2012

PHILADELPHIA, TUESDAY, MAY 7, 2013

An ALM Publication

Could Social Media Ruin Your Company?

BY JEREMY D. MISHKIN
Special to the Legal

The question is no longer whether your company should be involved with social media — it already is, whether you're leading or following. The skyrocketing popularity of these services is undeniable and the potential reward — for engaging, expanding and strengthening relationships with your key communities — is enormous. So are the risks. Risks come in many forms, and the prudent organization will assess its specific situation and take appropriate preventive steps to manage both risks created by others as well as risk created internally. Social media is a shockingly effective catalyst for both.

The key is understanding the nature of this new medium. The company and its counsel must be familiar not only with the rules, but with the culture of the online community. Social media is not just a new way to disseminate your message; it's a conversation taking place on a massively multi-person scale, worldwide. But just like any face-to-face conversation, it must be a two-way process (albeit on a massively multi-person scale) or it dies.

Here are the most frequent areas where companies can get in trouble, as well as some ideas for how to stay on the right side of the risk/reward curve.

REPUTATIONAL RISK

When you invite your customer, client or prospect to participate in a conversation, it would be lovely to think that you will only get standing ovations, but let's not kid ourselves. When you invite others into a conversation, you are also giving them permission to tell you something that you may not want to hear. Creating a Facebook page or a corporate Twitter feed are proven ways to engage your constituents and to make sure your voice is heard, but be aware that there will be times when people will vent their unhappiness. Even though you can (and should) control your pages, such as by monitoring and moderating comments, recognize that you cannot control everything. Feedback is the stock in trade for user-generated content sites like Yelp, Trip Advisor and Zagat (now owned by Google). If you're not watching your feedback on such public channels, you're missing an opportunity to gain important insights and, of equal importance, establish that you care about your customers and treat them with respect in how you handle the hard messages.

JEREMY D. MISHKIN *is a partner and chair of the litigation department of Montgomery, McCracken, Walker & Rhoads. His practice emphasizes commercial matters, technology, the Internet and First Amendment/media law issues. He is a member of the litigation section of the American Bar Association and was appointed in 2000 to the American Bar Association's Task Force on E-Commerce and Alternative Dispute Resolution.*

Sometimes, of course, the hard messages cross the line into true reputational harm. What can be done when your company is targeted with half-truths, misinformation and outright lies? In contrast with the traditional routes of suing for libel, social media presents different challenges and alters the standard risk-assessment decision tree in important ways:

- You may not know who made a particular statement.

For better or worse, many people who criticize prefer to do so while hiding behind a pseudonym. As a result, task number one is to figure out who is saying these terrible things about you — is it really a customer who got bad service or is it actually your major competitor who's trying to poison your search results? There are many ways to try to find the person behind the curtain and your best course of action may depend on who is speaking.

- The person may be acting irrationally because he or she is irrational.

Sometimes a person will decide that you're the one who's beaming messages directly into

his or her brain, despite his or her tinfoil pyramid hat. When you encounter one of these people, consider whether bringing legal action will make your position better or worse. Often, what they crave the most is attention. Sometimes, if you ignore them, they will get bored and leave you alone.

• Resist the temptation to sue a social media site for someone else's comment.

When you can't identify the person commenting, many clients believe they can just sue the site where the comment was made. However, in this country, such a claim would be barred by the Communications Decency Act (Section 230) as long as the medium did not create the offending message. This is true no matter how distasteful the message may be. (See, e.g., *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998); *Zeran v. America Online*, 129 F.3d 327 (4th Cir. 1997); *DiMeo v. Max*, 433 F. Supp. 2d 523 (E. D. Pa. 2006), aff'd., No. 06-3171 (3rd Cir., September 19, 2007).)

Here is the takeaway: There will be an untouchable amount of unpleasant or hostile chatter about anything, and that goes double for social media. You cannot stop the chatter, so rather than unleashing your litigation hounds, your best course — unpleasant as it may be — could be to just stay focused on your positive messages and wait for the nattering to die down. Putting out a fire with gasoline isn't usually effective.

INTELLECTUAL PROPERTY

Copying is fast and easy online and it's not always legal. What if someone steals your stuff? Or, what if someone posts something on your site that infringes others' rights? Standard reactions have proceeded down one of three paths: (1) ignore it; (2) fire off a threatening cease-and-desist-type letter; or (3) sue the person who stole and posted it.

Each of those classic responses carries risk, and some have been known to backfire badly. The fair-use doctrine is still alive and well and is zealously advocated online even if its parameters are a little fuzzy. (See *Lenz v. Universal Music*, 572 F. Supp. 2d 1150 (ND Cal. 2008), and subsequent opinion denying cross-motions for summary judgment dated January 24.) But more experienced users have discovered that there's now another alternative: use the event as an opportunity to engage and communicate with the community. An excellent recent example arose when the book *Broken Piano for President* was published with cover art that was pretty obviously inspired by the label on Jack Daniel's Whiskey. Rather than attempting to bully the publisher, the whiskey's lawyers used a more collaborative (some might say mellow) approach: "We are certainly flattered by your affection for the brand, but while we can appreciate the pop culture appeal of Jack Daniel's, we also have to be diligent to ensure that the Jack Daniel's trademarks are used correctly. ... As a fan of the brand, I'm sure that is not something you intended or would want to see happen."

By recognizing the nature of the social media, the company was able to simultaneously protect its legal rights and endear itself to the online world. That degree of understanding paid off enormously, as the company's cease-and-desist letter promptly went viral and garnered universal accolades from the online community.

Of course, you need to protect yourself online, as well, and it's easy for an unknown user to post infringing content in a comment or forum. Fortunately, there's an app for that — the Digital Millennium Copyright Act, 17 U.S.C. §512, provides that you cannot be held liable for someone else's active infringement as long as you follow the rules. Your attorney can help you make sure you're qualifying for the "safe harbor."

HACKING YOUR SYSTEM

War Games was a fun movie, but it also drove the enactment of one of the most far-reaching laws relating to computer systems — the Computer Fraud and Abuse Act. The CFAA is a powerful weapon in civil litigation and for prosecutors. It is so malleable that you need to bear it in mind as you navigate the social networks. Essentially, the CFAA provides that if someone gains access to a protected computer (defined as any computer connected to other computers, or, in today's world, pretty much every computer) without authorization and causes more than $5,000 in loss, he or she can be found liable. That's a pretty low threshold, especially for an offense that carries substantial risks.

Recent examples of the CFAA in action have included a young man who plugged his laptop into a computer at a university where he was not a student and obtained large numbers of academic articles. He was charged criminally and faced a possible 30-plus years in prison if he were to have been convicted. The trial will never take place, because the young man committed suicide right before jury selection was to start in *U.S. v. Swartz*, Crim. No. 11-10260, (D. Mass. 2011).

In another case, startlingly similar to the plot of *War Games*, a young man figured out that he could access email addresses of iPad users on a site maintained by their wireless network. He provided a list of the emails as proof that he could do so to the press, and was charged with violating the CFAA. A jury convicted him and he is presently appealing on the grounds that however vague the law may be, it cannot be read to criminalize accessing a publicly available website. That case is *U.S. v. Auernheimer*, Crim. No. 11-470 (D.N.J. 2012).

SECURITIES FRAUD

The ease and speed with which someone can tweet or post an update has created particular challenges for the investment world, which is constantly seeking the latest and best information in order to make profitable trades. At the same time, public companies must abide by the Securities and Exchange Commission's Regulation FD, requiring that when they provide information to the investing public they do so uniformly and not play favorites.

So what happens when a company executive uses his or her own social media channel to comment about the company business? Can something as simple as a 140-character blurb lead to an SEC investigation? Of course it can — just as any other communication by someone with insider status could. A Netflix executive posted an update on his own Facebook page about how much video the company had streamed, even though the company itself did not make a formal announcement of that milestone. Whether Regulation FD was applicable to this sort of situation was resolved on April 2, when the SEC issued Release 2013-51. The SEC decided not to pursue enforcement proceedings against Netflix, but a smart company will now take affirmative steps to prevent its executives from crossing that line.

PROTECTING AGAINST RISK

Social media continues to reach more people, more personally, every day than any other form of communication ever has. Companies that understand their legal rights and protect against their legal risks in harmony with the standards of the connected online community will reap enormous rewards. •